Strengthening Regulations Governing Use of Portable Media

Captain Stuart C. Smith Jr.

Major Amy B. Irvin

20 February 2009

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
20 FEB 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Strengthening Regulations Governing Use of Portable Media	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps Combat Development Command,Marine Corps University, 2076 South Street,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

INTRODUCTION

Twenty-first century man lives in a world in which eight gigabytes (GB) of data can be stored on a device with dimensions of a little more than three centimeters by a little more than one centimeter. This device weighs less than six grams, costs less than twenty-four dollars, is highly portable, widely available, and easily accessible using a universal serial bus (USB) interface. These devices are also referred to as thumb drives, flash media, USB flash drives, memory sticks, removable storage media[1], or portable media. Although incredibly useful at home or work, they pose a significant risk. This form of media can easily be lost, stolen, or compromised. It can also be used to introduce, intentionally or unintentionally, malicious code and to infect a targeted system or series of systems on any given network.

As technology develops at such a rapid pace, often emerging solutions become mainstream before sufficient testing is completed to determine risks associated with a new product. Additionally, users are so enamored with the convenience of a new solution that they ignore the dangers connected with its use. Such is the case within the Department of Defense (DoD). Military regulations governing the use of portable media must be strengthened to prevent compromise by improving training and

awareness, limiting individual discretion, and imposing stiff penalties when violations occur.

HISTORICAL BACKGROUND

When personal computers first became popular and affordable, the portable media of the day was a five and a quarter-inch floppy disk. With improvements in technology and a demand for greater storage capacity, the three and half-inch floppy dominated the market in portable media for several years. The most common were capable of storing up to 2.88 MB. After about ten years of mainstream service, the floppy disk was replaced by compact disks (CDs). The most common CDs are capable of storing 680 MB of data. After CDs, digital versatile discs (DVDs) became an attractive option. DVD storage capacity varies between 4.7 GB and 17 GB. In 2000, when thumb drives were introduced, they were only capable of 8 MB of storage. Eventually, with advances in technology, 64 MB became available, then 128 MB, 256 MB, 512 MB, 1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32GB, and now 64 GB. Other portable devices are capable of storing data-at-rest (DAR);[2] external hard drives are the most common, which are capable of storing terabytes of data.

In March 2006, MARADMIN 143/06 was released notifying, "...enlisted Marines, active and reserve, on active duty between January 2001 and December 2005 of the loss of Privacy Act

information." The "...thumb drive contained Privacy Act data to include, name, social security number, marital status, and enlistment contract information."[3] In April 2006, the *New York Times* reported, "American investigators have paid thousands of dollars to buy back the stolen drives, according to shopkeepers outside the major military base here..."[4]

In response to these reported incidents, and many others, MARADMIN 348/06 was released stating, "Privacy Act data will not be stored on a removable storage device, thumb drive, floppy, CD-ROM, DVD, or laptop unless encrypted and password protected."[5] Additionally, "Privacy Act data will not be maintained on personal computers/devices."[5]

In July 2007, ALNAV 057/07 was released indicating, "during the past 18 months, the DoN has reported over 100 incidents involving the loss of PII[6], impacting over 200,000 Navy and Marine Corps personnel, including retirees, civilians, and their dependents. The most common causes of loss/compromise have been the loss or theft of laptop computers, thumb drives, and other portable removable media."[7]

In response to these documented reports of sensitive data being lost, stolen or compromised, the DoD Chief Information Officer (CIO) revised policy governing portable media in July 2007 to include the following statement:

> All unclassified data at rest that has not been approved for public release and is stored on mobile computing devices such as laptops and personal digital assistants (PDAs) or removable storage media such as thumb drives and compact discs, shall be treated as sensitive data and encrypted using commercially available encryption technology. Minimally, the cryptography shall be National Institute of Standards and Technology (NIST) Federal Information Processing Standard 140-2 (FIPS 140-2) compliant...[8]

This statement essentially requires sufficient encryption on all mobile computing devices, whether it contained Privacy Act data or not.

Nonetheless, as result of ineffective policy, poor enforcement, and several instances of lost, stolen and compromised data, effective 18 November 2008, and in accordance with Marine Corps Enterprise Network (MCEN) Operational Directive 293-08, "all MCEN users must immediately suspend use of memory sticks, thumb drives and camera flash memory cards on all classified and unclassified USMC networks until further notice." [9] However, this directive does not prohibit the use of

external hard drives that perform a function similar to memory sticks.

IMPROVING TRAINING AND AWARENESS

One area in which significant progress must be made is training and awareness. The danger associated with using portable media is not resonating with the average service member. According to DoDD 8570.1, Information Assurance Training, Certification, and Workforce Management, dated 15 Aug 2004, "...requires annual information assurance training."[10]

Per paragraph 4.2.5.4.1. of SECNAV M5239.1, dated November 2005, "IA training shall be monitored and reported as an element of mission readiness and as a management review item. The status of awareness and training provision and certifications shall be reported to DON CIO as an element of mission readiness." [11]

For the average service member, by established policy our military training consists of personally identifiable information (PII)[12] training and information assurance (IA)[13] training. These requirements are typically completed via an online computer-based training module. Although computer-based training has come a long way, more attention must be devoted to this particular subject.

Refresher training for users is mandatory once a year, but this is insufficient. Three methods of inoculating the user

population with information regarding portable media include expressed, implied, and informed consent. Expressed consent is satisfied by signing an end user agreement, which details regulations governing the use of DoD information systems. Service members typically complete an end user agreement before access is granted to a particular system. Implied consent is satisfied by the DoD warning banner. MARADMIN 714/07, dated 6 December 2007, modifies the DoD warning banner. Unfortunately, many users are so accustomed to the DoD warning banner, they are prepared to click, "Ok," before the text box appears on the screen. Informed consent is satisfied by completing the computer-based training modules.

One example of a routine violation includes a recent email received from a senior officer which contained social security numbers for more than two dozen commissioned officers from three different services. The purpose of the email was to provide a roster; however, social security numbers were unnecessary.

Although intrusive and manpower intensive, a return to classroom instruction with a low student to teacher ratio is necessary in order to impart the risks associated with the use of portable media effectively, and to instruct users about safe methods to store data at rest.

LIMITING INDIVIDUAL DISCRETION

Until recently, DoD policy governing portable media, although strict, allowed for significant individual discretion. Few checks and balances and limited technical enforcement existed. Unfortunately, when a perceived operational necessity presents itself, a service member will often knowingly or unknowingly compromise policy and place sensitive, unauthorized material on portable media with or without approved encryption. This results in convenience becoming the rule of the day at the risk of personal information being exposed to unauthorized recipients.

In April 2006 in Bagram, Afghanistan thumb drives were stolen on multiple occasions from U.S. forward operating bases and sold in local Afghani markets. Information retrieved from these devices included content classified at the secret level, photos, and phone numbers of people described as Afghan spies working for the U.S. military, as well as social security numbers and names of U.S. service members.[14]

An example of a strict policy can be found at the Gray Research Center (GRC). Although the GRC is not part of the Marine Corps Enterprise Network (MCEN), it does fall under DoD. The GRC restricts USB ports by introducing a physical barrier to the port. Although the port is not technically disabled, users

are unable to use targeted USB ports because a device prohibits physical connection. The only two USB ports in use are for the keyboard and mouse.

IMPOSING STIFF PENALTIES

Military leadership is a significant part of the problem. Often, military leadership encourages violations as they are unaware of the consequences or policy governing portable media. As with all facets of leadership, uniformed leaders must lead by example with regard to the use of portable media.

As it stands, current policies are routinely violated by members of all ranks. Common violations include using personal thumb drives to store PII, failing to use approved encryption software to protect PII, using thumb drives to transfer self-approved content from a network with a higher classification to a network with a lower classification, and, as of December 2008, using any thumb drive on any Marine Corps network.

When violations occur, stiff penalties are called for. Otherwise, the policy will have no traction within the military community.

COUNTERARGUMENTS

Many believe the risk of compromise is limited. These users believe that limiting discretion will only stifle initiative and create an additional burden on an already

overburdened workforce. While this policy will create an additional burden, but just like wearing a seatbelt in the car, it is a necessary burden in order to preserve the force. The alternative has far worse consequences.

CONCLUSION

Learning, following, and enforcing portable media policy is a force protection measure. Additional effort must be made to prevent compromising sensitive data. The consequence of data at rest getting into the hands of the enemy gives them a marked advantage. Plausible results range from strategic implications to loss of life. Lost portable media containing sensitive information in custody of an insurgent is equally as dangerous as the pull of a trigger from an enemy’s well-aimed service weapon.

GLOSSARY

Removable Storage Media - Refers to cartridge and disc-based removable and portable storage media devices that can be used to easily move data between computers. Examples of removable storage media include, but are not limited to, floppy disks, compact discs, USB flash drives, external hard drives, portable media, and other flash memory cards/drives that contain non-volatile memory. See DoD Memorandum, 3 July 2007.

Data-at-rest (DAR) – Any data residing on hard drives, thumb drives, laptops, etc. In some cases, this data can be Controlled Unclassified Information or it can be what's called FOUO, For Official Use Only. It can be called Critical Program Information, CPI; or it can be called Personally Identifiable information. Encrypting data at rest will strengthen our security posture and mitigate the impact of lost or stolen data. See DoN CIO DAR FAQ, 26 September 2007.

Personally Identifiable Information (PII) – Any information that can be used to distinguish or trace an individual's identity, such as his or her name or social security number, alone, or when combined with other identifying information that is linkable to a specific individual, such as date, a place of birth, or mother's maiden name. See DoN CIO DAR FAQ, 26 September 2007.

Information Assurance (IA) - Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. See SECNAV M5239.1.

NOTES

1. See Glossary

2. See Glossary

3. MARADMIN 143/06, *Lost Privacy Act Data,* 24 March 2006.

4. Carlotta Gall, “U.S. Investigates Sale of Secret Data in Afghan Market,” New York Times, 13 April 2006, sec. A.

5. MARADMIN 348/06, *Use of Data Protected by the Privacy Act,* 26 July 2006.

6. See Glossary

7. ALNAV 057/07, *Safeguarding Personally Identifiable Information (PII) from Unauthorized Disclosure,* July 2007.

8. Department of Defense Memorandum, *Encryption of Sensitive Unclassified Data at Rest on Mobile Computing,* 03 July 2007.

9. MCNOSC User Alert email, *Immediate Suspension of Thumb Drives, Memory Sticks, and Camera Flash Memory,* 18 November 2008.

10. DoDD 8570.1, *Information Assurance Training, Certification, and Workforce Management*, 15 Aug 2004.

11. Department of Navy, Secretary of the Navy Manual 5239.1, *Department of the Navy Information Assurance (IA) Policy,* 20 December 2004.

12. See Glossary

13. See Glossary

14. Carlotta Gall, “U.S. Investigates Sale of Secret Data in Afghan Market,” New York Times, 13 April 2006, sec. A.

BIBLIOGRAPHY

All Navy Message (ALNAV) 057/07, *Safeguarding Personally Identifiable Information (PII) from Unauthorized Disclosure,* July 2007. Washington, D.C.

All Navy Message (ALNAV) 070/07, *Department of the Navy (DON) Personally Identifiable Information (PII) Annual Training Policy,* 4 October 2007. Washington, D.C.

Carlotta Gall, "U.S. Investigates Sale of Secret Data in Afghan Market," *New York Times*, 13 April 2006, sec. A.

Commandant of the Marine Corps, All Marine Message 143/06, *Lost Privacy Act Data,* 24 March 2006. Washington D.C.

Commandant of the Marine Corps, All Marine Message 348/06, *Use of Data Protected by the Privacy Act,* 26 July 2006. Washington D.C.

Commandant of the Marine Corps, All Marine Message 714/07 *Mandatory Requirement to Use Standard Department of Defense Information Systems (IS) Consent Banner and User Agreement,* 6 December 2007. Washington D.C.

Commandant of the Marine Corps, All Marine Message 732/07, *Data at Rest Encryption for Mobile Computing Devices and Removable Storage Media*, 14 December 2007. Washington D.C.

Commandant of the Marine Corps, All Marine Message 333/08, *Mandatory Requirement to Use Standard Department of Defense Information Systems (IS) Consent Banner and User Agreement,* 5 June 2008. Washington D.C.

Commandant of the Marine Corps, All Marine Message 647/08, *Immediate Discontinued Use of Removable Flash Media Storage and Memory Devices on Marine Corps Networks,* 20 November 2008. Washington D.C.

Commandant of the Marine Corps, All Marine Message 692/08, *Department of Defense Warning Banner and User Agreement,* 3 December 2008. Washington D.C.

Department of Defense Directive 8570.1, *Information Assurance Training, Certification, and Workforce Management*, 15 Aug 2004. Washington, D.C.

Department of Defense Memorandum, *Withholding of Personally Identifying Information under the Freedom of Information Act (FOIA),* 9 November 2001. Washington, D.C.

Department of Defense Memorandum, *Protection of Sensitive Department of Defense (DoD) Data at Rest on Portable Computing Devices,* 18 April 2006. Washington, D.C.

Department of Defense Memorandum, *Encryption of Sensitive Unclassified Data at Rest on Mobile Computing,* 03 July 2007. Washington, D.C.

Department of Defense Memorandum, *Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media,* 19 March 2008. Washington, D.C.

Department of Navy, Secretary of the Navy Manual 5239.1, *Department of the Navy Information Assurance (IA) Policy,* 20 December 2004. Washington, D.C.

Department of Navy, Secretary of the Navy Instruction 5239.3A, *Information Assurance Manual,* November 2005. Washington, D.C.

Department of Navy, Chief Information Officer Message, *DON Encryption of Sensitive Unclassified Data at Rest Guidance,* 09 October 2007. Washington, D.C.

Major Bret M. Hyla, S3 Future Operations Officer, Marine Corps Network Operations and Security Center (MCNOSC), 703-432-6853

MCNOSC User Alert email, *Immediate Suspension of Thumb Drives, Memory Sticks, and Camera Flash Memory,* 18 November 2008.

Word Count: 1657